

DMP:JAM/ADR/MS  
F. #2019R01707

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA

- against -

VADIM YERMOLENKO,

Defendant.

----- X

THE GRAND JURY CHARGES:

### INTRODUCTION

At all times relevant to this Superseding Indictment, unless otherwise indicated:

I. The Defendant and the Serniya Procurement Network

1. The defendant VADIM YERMOLENKO was a dual citizen of the United States and the Russian Federation who resided in New Jersey.

2. OOO<sup>1</sup> Serniya Engineering (“Serniya”) was a wholesale machinery and equipment company based in Moscow, Russia. Serniya headed an illicit procurement

---

<sup>1</sup> “OOO” is the abbreviation for the Russian business entity type, “общество с ограниченной ответственностью,” which means limited private company and is roughly the equivalent of a limited liability company or LLC in the United States.

FILED  
IN CLERK’S OFFICE  
U.S. DISTRICT COURT E.D.N.Y.  
\* SEPTEMBER 30, 2024 \*  
BROOKLYN OFFICE

### S U P E R S E D I N G I N D I C T M E N T

Cr. No. 22-409 (S-3) (HG)  
(T. 18, U.S.C., §§ 371, 554(a),  
981(a)(1)(C), 982(a)(2), 982(b)(1),  
1344, 1349, 1956(h), 2 and 3551 et  
seq.; T. 21, U.S.C., § 853(p); T. 28,  
U.S.C., § 2461(c); T. 50, U.S.C.,  
§§ 4819(a)(1), 4819(a)(2)(A)-(G),  
4819(b), 4819(d)(1), 4819(d)(2); T. 15,  
C.F.R., §§ 736.2(b)(1) and 746.8(a)(1))

network operating under the direction of Russia's intelligence services (collectively, the "Serniya Network"), which evaded U.S. and Western sanctions to acquire sensitive military-grade and dual-use technologies, including advanced semiconductors, for the Russian military, defense sector and research institutions. The Serniya Network's clients included the following Russian companies and entities: State Corporation Rostec, the state-owned defense conglomerate; State Atomic Energy Corporation Rosatom ("Rosatom"); JSC Rusnano, the state-owned nanotechnology company; the National Research Nuclear University of the Moscow Engineering Physics Institute ("MEPhI"); the Ministry of Defense; the Foreign Intelligence Service ("SVR"); and various components of the Federal Security Service ("FSB"), Russia's principal security agency and the main successor agency to the Soviet Union's KGB, including the Department of Military Counterintelligence and the Directorate for Scientific and Technological Intelligence, commonly known as "Directorate T."

3.      OOO Sertal ("Sertal") was a wholesale machinery and equipment company based in Moscow, Russia. As described herein, Sertal operated within the Serniya Network and in turn utilized a network of front companies, shell entities and bank accounts throughout the world, including in the United States, to source, purchase and ship export-controlled items from the U.S. to Russia.

4.      Sertal was an FSB-accredited contractor authorized to conduct highly sensitive and classified procurement activities. In on about August 2020, Sertal obtained a renewal of its license from the FSB, allowing it to "carry out work related to the use of

information constituting a state secret up to the top-secret level.”<sup>2</sup> In an August 31, 2020 letter to the All-Russian Research Institute of Automation (“VNIIA”), a Rosatom subsidiary that developed strategic and tactical nuclear weapons and was responsible for Russia’s nuclear stockpile, Sertal’s General Director confirmed the reissuance of its FSB license, stating that, “since June 2016, Sertal LLC has successfully performed and is performing work using information constituting a state secret . . . we suggest that you further consider our company as a potential supplier of complex equipment, devices and components.”

5. On or about March 3, 2022, Serniya and Sertal were added to the U.S. Department of Commerce (“DOC”) Bureau of Industry and Security (“BIS”) Entity List (the “Entity List”), found at Title 15, Code of Federal Regulations, part 774, Supplement Number 4. The Entity List imposed additional license requirements and export restrictions due to a determination that the entities included on the list had engaged in activities contrary to U.S. national security or foreign policy interests. BIS added Serniya and Sertal to the Entity List because of their relationship to the Russian government and in response to Russia’s invasion of Ukraine beginning in February 2022. Specifically, BIS indicated that Serniya, Sertal and other entities were sanctioned because they “have been involved in, contributed to, or otherwise supported the Russian security services, military and defense sectors, and military and/or defense research and development efforts.” 87 Fed. Reg. 13141 (Mar. 9, 2022). BIS adopted a “policy of denial” with respect to Serniya and Sertal, indicating that BIS would not authorize a license to export items to Serniya or Sertal.

---

<sup>2</sup> Unless otherwise indicated, all quoted communications contained herein are translations of written or spoken Russian.

6. On or about March 31, 2022, pursuant to Executive Order 14024, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") designated Serniya, Sertal and several other entities in the Serniya Network and added them to the list of Specially Designated Nationals and Blocked Persons (the "SDN List"). According to OFAC's press release, the designation was part of "its crackdown on the Kremlin's sanctions evasion networks and technology companies, which are instrumental to the Russian Federation's war machine." OFAC described Serniya as:

the center of a procurement network engaged in proliferation activities at the direction of Russian Intelligence Services. This network operates across multiple countries to obfuscate the Russian military and intelligence agency end-users that rely on critical western technology. Serniya and Moscow-based OOO Sertal work to illicitly procure dual-use equipment and technology for Russia's defense sector.

7. OFAC also designated several individuals and companies operating in the Serniya Network, including United Kingdom-based Majory LLP, United Kingdom-based Photon Pro LLP, and Spain-based Invention Bridge SL, among others, identifying them as "front companies utilized by Serniya to facilitate its procurement of key equipment for the Government of the Russian Federation."

## II. The Statutory and Regulatory Background

### A. The International Emergency Economic Powers Act and the Relevant Sanctions Orders and Regulations Relating to Russia

8. The International Emergency Economic Powers Act ("IEEPA"), codified at Title 50, United States Code, Sections 1701 through 1708, conferred upon the President the authority to deal with unusual and extraordinary threats to the national security and foreign policy of the United States. Section 1705 provided, in part, that "[i]t shall be

unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this chapter.” 50 U.S.C. § 1705(a).

9. In 2014, pursuant to his authorities under the IEEPA, the President issued Executive Order 13660, which declared a national emergency with respect to Russia’s violation of the sovereignty of Ukraine by asserting authority over the Crimea region. To address this national emergency, the President blocked all property and interest in property that were then or thereafter came within the United States or the possession or control of any United States person, of individuals determined by the Secretary of the Treasury to meet one or more enumerated criteria. These criteria included, but were not limited to, individuals determined to be responsible for or complicit in, or who engaged in, actions or policies that threatened the peace, security, stability, sovereignty or territorial integrity of Ukraine; or who materially assisted, sponsored or provided financial, material or technological support for, or goods or services to, individuals or entities engaging in such activities. Executive Order 13660 prohibited, among other things, transferring, paying, exporting, withdrawing and otherwise dealing in any interest in property in the United States owned by a person whose property and interests in property were blocked (a “blocked person”), as well as the making of any contribution or provision of funds, goods or services by a United States person to or for the benefit of a blocked person and the receipt of any contribution or provision of funds, goods or services by a United States person from any such blocked person.

10. The national emergency declared in Executive Order 13660 with respect to the situation in Ukraine remained in continuous effect since 2014 and was renewed on March 2, 2022, following Russia’s most recent invasion of Ukraine.

11. On multiple occasions, the President expanded the scope of the national emergency declared in Executive Order 13660, including through: (1) Executive Order 13661, issued on March 16, 2014, which addressed the actions and policies of the Russian Federation with respect to Ukraine, including the deployment of Russian Federation military forces in the Crimea region of Ukraine; and (2) Executive Order 13662, issued on March 20, 2014, which addressed the actions and policies of the Government of the Russian Federation, including its purported annexation of Crimea and its use of force in Ukraine. Executive Orders 13660, 13661 and 13662 were collectively referred to as the “Ukraine-Related Executive Orders.” On February 21, 2022, the President again expanded the scope of the national emergency, finding that the Russian Federation’s purported recognition of the so-called Donetsk People’s Republic and Luhansk People’s Republic regions of Ukraine contradicted Russia’s commitments under the Minsk agreements and threatened the peace, stability, sovereignty and territorial integrity of Ukraine.

12. The Ukraine-Related Executive Orders authorized the Secretary of the Treasury to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President under the IEEPA, as necessary to carry out the purposes of those orders. The Ukraine-Related Executive Orders further authorized the Secretary of the Treasury to redelegate any of these functions to other offices and agencies of the U.S. Government.

13. To implement the Ukraine-Related Executive Orders, OFAC issued certain Ukraine-Related Sanctions Regulations. These regulations incorporated by reference the prohibited transactions set forth in the Ukraine-Related Executive Orders. See 31 C.F.R. § 589.201. The regulations also provided that the names of persons designated directly by

the Ukraine-Related Executive Orders, or by OFAC pursuant to the Ukraine-Related Executive Orders, whose property and interests were therefore blocked, would be published in the Federal Register and incorporated into the SDN List, published on OFAC's website. Id. n.1.

B. The Export Control Reform Act and Export Administration Regulations

14. The Export Administration Regulations ("EAR"), 15 C.F.R. §§ 730-774, were promulgated by BIS to regulate the export of goods, technology and software from the United States. Under the Export Control Reform Act ("ECRA"), it was a crime to violate, attempt to violate, conspire to violate or cause a violation of any regulation, order, license or authorization issued pursuant to the statute, including the EAR. See 50 U.S.C. § 4819(a)(1). Willful violations of the EAR constituted criminal offenses under the ECRA, and carried a 20-year maximum term of imprisonment and up to a \$1,000,000 fine. See 50 U.S.C. § 4819(b).

15. Through the EAR, BIS reviewed and controlled the export from the United States to foreign countries of certain U.S. items. See 15 C.F.R. §§ 734.2-.3. In particular, BIS placed restrictions on the export and re-export of items that it determined could make a significant contribution to the military potential or nuclear proliferation of other nations or that could be detrimental to the foreign policy or national security of the United States. Under the EAR, such restrictions depended on several factors, including the technical characteristics of the item, the destination country, the end user and the end use of the item.

16. The most sensitive items subject to the EAR controls were identified on the Commerce Control List ("CCL") set forth in Title 15, Code of Federal Regulations, part

774, Supplement Number 1. Items listed on the CCL were categorized by Export Control Classification Number (“ECCN”), each of which was subject to export control requirements depending on destination, end use and end user of the item.

17. BIS published the names of certain foreign persons—including businesses, research institutions, government and private organizations, individuals and other types of legal persons—that were subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items. These persons comprised the Entity List. The persons on the Entity List were subject to individual licensing requirements and policies supplemental to those found elsewhere in the EAR, due to a determination that such persons had engaged in activities contrary to U.S. national security and/or foreign policy interests.

18. In response to Russia’s 2022 invasion of Ukraine, the DOC imposed new license requirements on exports to Russia. As of February 24, 2022, any item classified under any ECCN in Categories 3 through 9 of the CCL required a license to be exported to Russia. See 87 Fed. Reg. 12226 (Mar. 3, 2022). As of April 8, 2022, the license requirement for export to Russia was expanded to cover all items on the CCL. See 87 Fed. Reg. 22130 (Apr. 14, 2022). These rules were codified in Title 15, Code of Federal Regulations, part 746.8, which stated, “a license is required, excluding deemed exports and deemed reexports, to export, reexport, or transfer (in-country) to or within Russia or Belarus any item subject to the EAR and specified in any Export Control Classification Number (ECCN) on the CCL.”



### III. Overview of the Criminal Scheme

19. Since at least 2017, the defendant VADIM YERMOLENKO and his co-conspirators in the Serniya Network unlawfully sourced, purchased and shipped millions of dollars in military and sensitive dual-use technologies from U.S. manufacturers and vendors located in the Eastern District of New York and elsewhere (collectively, the “U.S. Companies”) for Russian end users, in violation of IEEPA, ECRA and other U.S. criminal statutes. These items included advanced electronics and sophisticated testing equipment used in quantum computing, hypersonic and nuclear weapons development and other military and space-based military applications.

20. To effectuate the scheme, the defendant VADIM YERMOLENKO and his co-conspirators made and caused to be made material misrepresentations and omissions, both orally and in writing, with respect to invoices, end use statements, financial records and shipping documents, among other items, to conceal the nature of these illicit procurement transactions. By doing so, YERMOLENKO and his co-conspirators caused the U.S. Companies to sell and export sensitive military and dual-use items in violation of IEEPA, ECRA, and other U.S. laws and regulations; process and accept payments in furtherance of such illicit transactions; and fail to file documents with the DOC, BIS and other U.S. government entities, including license applications and required statements regarding the ultimate consignee and purchaser. YERMOLENKO and his co-conspirators also caused U.S. financial institutions to process millions of dollar-based payments in violation of IEEPA, ECRA and other U.S. laws and regulations. Several of these transactions were processed through correspondent accounts at New York City banks and within the Eastern District of New York.

21. To purchase and export items from the U.S. Companies, the defendant VADIM YERMOLENKO and his co-conspirators routed and layered transactions through a variety of front companies and bank accounts located in jurisdictions throughout the world. Some of these front companies and bank accounts were created and used by YERMOLENKO.

22. Specifically, items were shipped from the U.S. Companies to various locations in the United States and Europe that corresponded to addresses registered to front companies controlled by the Serniya Network. Items were then repackaged and reshipped to several intermediate locations in Europe and Asia before arriving in Russia. Common transshipment points included locations in Estonia, Finland, Germany, the Netherlands and Hong Kong. Additionally, shipping documents understated the value of the exports from the U.S. to avoid applicable reporting requirements, thereby avoiding additional scrutiny.

23. In these ways, the defendant VADIM YERMOLENKO and his co-conspirators disguised the audit trail of shipments and payments and concealed the true Russian end users for items purchased from the U.S. Companies.

#### IV. The Defendant's Involvement in the Serniya Network

24. The defendant VADIM YERMOLENKO worked directly with Co-Conspirator-1 ("CC-1"), an individual whose identity is known to the Grand Jury, in unlawfully exporting dual-use and controlled items from the United States. CC-1, who spoke English, communicated with the U.S. Companies through in-person meetings, telephonic conversations and in email and text exchanges to purchase items requested by Russian end users. In those communications, CC-1 misrepresented and omitted material

information, including information about how the items would be used, the various parties involved in the transactions, and the identities of the ultimate Russian end users.

25. At CC-1's direction, the defendant VADIM YERMOLENKO shipped packages to Co-Conspirator-2 ("CC-2"), an individual whose identity is known to the Grand Jury, at CC-2's residence in Merrimack, New Hampshire (the "New Hampshire Residence"), which was a frequent transshipment point for items that were unlawfully exported from the United States to Russia. For example, regarding one shipment, CC-1 instructed YERMOLENKO, "We need to send DHL to Germany, to the same company" with the items' description listed as "Duffle bag size L -\$300" and "Duffle bag size XL - \$550." YERMOLENKO sent CC-1 a shipping invoice that YERMOLENKO had signed addressed to the New Hampshire Residence. CC-1 then forwarded the invoice to co-conspirators in the Serniya Network based in Russia, who had placed the order for "Military Unit 33949," a part of the SVR.

26. In July 2022, CC-1 attempted to purchase a \$15,564 3 GHz signal generator controlled by the DOC under ECCN 3A992.a for reasons of anti-terrorism, from an Illinois-based test equipment company (the "Illinois Company"), an entity the identity of which is known to the Grand Jury. In an email dated July 25, 2022, CC-1 requested that an employee at the Illinois Company "please ship the generator to our NH address" for "Strandway LLC," and provided the address of the New Hampshire Residence. CC-1 also provided the Illinois Company with a pro forma invoice and a Form BIS-711 ("Statement by Ultimate Consignee and Purchaser")—an end use statement filed with the DOC—falsely listing Strandway LLC at the New Hampshire Residence as the "ultimate consignee and purchaser." The Form BIS-711 was signed by the defendant VADIM YERMOLENKO,

who was listed as the “Director” of Strandway LLC, and certified that the signal generator would not be “reexported or incorporated into an end product.”

27. The defendant VADIM YERMOLENKO was aware that the items that he and his co-conspirators were acquiring and exporting to end users in Russia were not permitted to be exported to Russia. For example, a message from YERMOLENKO to CC-1 on October 29, 2018 attached an invoice from the U.S. branch of a Taiwanese technology conglomerate that listed YERMOLENKO as the exporter from a New Jersey address and stated that the item was:

controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

28. Additionally, the defendant VADIM YERMOLENKO altered or destroyed shipping documents and other business records to conceal the illicit transactions in which he engaged. For example, in a May 23, 2018 email to YERMOLENKO, CC-1 instructed “[b]efore sending, you need to ask your people to open the box, take a picture and send it to me—the part itself, on both sides and the invoice that is attached. To be sure that they sent exactly what we ordered. Throw away the original invoice and DO NOT send it to Germany!”

29. The defendant VADIM YERMOLENKO and CC-1 also established and managed numerous front companies in the United States, including entities in the Eastern District of New York, in furtherance of the scheme. Specifically, CC-1 used agents

and nominees—including YERMOLENKO—to create fictitious corporate entities and obtain corresponding Employer Identification Numbers (“EIN”) from the Internal Revenue Service (“IRS”). In this manner, CC-1 and YERMOLENKO created the following entities, several of which were incorporated with addresses in the Eastern District of New York: Crossgate LLC; Divatek Trading Inc.; Fennica Networks LLC; JJ Networks LLC; Strand Networks LLC; Squareweb LLC; Trailgate Systems LLC; and Windwire Technologies LLC. YERMOLENKO registered some of these entities in his wife’s name.

30. Because the defendant VADIM YERMOLENKO, CC-1 and their co-conspirators concealed the ownership, control and purpose of these front companies, the IRS was unable to properly assess any income generated in the U.S. by YERMOLENKO, CC-1 and others. For example, despite Strand Networks LLC receiving over \$6.2 million in gross receipts between 2020 and 2022, Strand Networks LLC has never filed a business tax return, nor has YERMOLENKO ever included Strand Networks LLC on Schedule C of his personal income tax returns. Indeed, business tax returns have never been filed for Crossgate LLC, Fennica Networks LLC, JJ Networks LLC, Squareweb LLC, Trailgate Systems LLC or Windwire Technologies LLC, and most of those entities have never appeared on the Schedule C for YERMOLENKO or his wife.

31. The defendant VADIM YERMOLENKO and CC-1 also opened numerous bank accounts in the names of these front companies (the “U.S. Bank Accounts”) at Bank 1, Bank 2, Bank 3 and Bank 4, entities the identities of which are known to the Grand Jury. CC-1 directed YERMOLENKO to manage the U.S. Bank Accounts and conduct certain transactions on behalf of the Serniya Network. In exchange for doing so, CC-1 paid YERMOLENKO thousands of dollars per month. For example:

(a) In or about 2019, YERMOLENKO provided CC-1 with YERMOLENKO's wife's signature to use on IRS documents for company applications and applications to open U.S. Bank Accounts.

(b) In an August 1, 2019 email to CC-1, YERMOLENKO stated, "[W]e need docs for all companies, tomorrow I'm going to open accounts." CC-1 responded by sending a list of IRS, state and other official documents for four front companies, including Strand Networks LLC and Trailgate Systems LLC.

(c) In an email on August 5, 2019, YERMOLENKO provided CC-1 with the account names, electronic logins, passwords and answers to the security questions for the bank accounts of five different front companies, including Strand Networks LLC and Trailgate Systems LLC. Notably, several invoices exchanged amongst co-conspirators in the Serniya Network listed Strand Networks LLC as the beneficiary.

(d) In a series of April 2022 emails, CC-1 instructed YERMOLENKO as follows: "Here is the document of the new NJ LLC and EIN. You can open an account. Let's start with [Bank 1]. If they open an account there, then ask them if it is possible to have an account with access to their CEO Portal, where wire functionality and double custody with 2 RSA tokens . . . and wire limits to at least \$50k/wire and \$200-300k/months." On April 26, 2022, YERMOLENKO opened an account in the name of "JJ Networks LLC" at a Bank 1 branch in New Jersey. The following day, YERMOLENKO deposited a check for \$44,400.84 and immediately transferred \$9,353 to Strandway LLC, and \$34,000 to Trailgate Systems LLC, and withdrew the rest of the balance in cash.

(e) In an April 29, 2022 email, CC-1 instructed YERMOLENKO, "You need to call, or, which would be better, go to [the bank] – you need to find out why

they won't send the outgoing wire transfer to Iceland from Strand Networks LLC . . . if the bank asks what the payment is for – for bicycle spare parts, sporting goods and textile products.” The email attached an invoice describing the cargo as deep-sea navigation and communications equipment.

(f) In a June 15, 2022 message exchange, CC-1 asked CC-2, “Is it possible for you to send my Wells Fargo token via Fedex to Vadik [a reference to YERMOLENKO] in NJ?” CC-1 then sent YERMOLENKO's home address to CC-2 and asked CC-2 to “send it today.”

32. This use of front companies and nominee accounts enabled the defendant VADIM YERMOLENKO and CC-1 to move money while preventing the IRS from assessing or receiving taxes due on any income. In electronic communications, YERMOLENKO and CC-1 discussed possible “issues with OFAC” involving the U.S. Bank Accounts and gave false and misleading information to U.S. financial institutions to ensure that wire transactions were completed.

33. On or about August 4, 2022, the defendant VADIM YERMOLENKO opened an account in the name of Strand Networks LLC with a United Kingdom-based financial technology company that provided global money transfer services (the “U.K. Strand Account”). That same day, YERMOLENKO and CC-1 discussed sending a “test” payment from the U.K. Strand Account and initiated a transfer of approximately \$100 to Co-Conspirator-3 (“CC-3”), an individual whose identity is known to the Grand Jury, in Estonia.

34. On or about October 17, 2022, approximately \$5,949 was sent from the U.K. Strand Account to a weapons and ammunition company based in Germany (the “German Company”). A review of records from the German Company reflected that this

payment was to purchase thousands of bullets manufactured by a Nebraska-based firearms components and manufacturing company (the “Nebraska Company”) and ship them to CC-3 in Tallinn, Estonia. These bullets were suitable for sniper rifles and other military firearms and controlled under ECCN 0A505.x for, among other things, reasons of national security and anti-terrorism.

35. On or about October 27, 2022, CC-3 was stopped by police and border guard officers in Narva, Estonia, where CC-3 was attempting to cross from Estonia into Russia. Inside of CC-3’s vehicle were approximately 35 different types of semiconductors and other electronic components, at least four of which were of U.S.-origin and controlled by the DOC under ECCN 3A992.a for reasons of anti-terrorism. One of the items had been purchased by CC-1 and shipped to CC-3 on or about October 18, 2022.

36. Also secreted in CC-3’s vehicle were thousands of bullets manufactured by the Nebraska Company. The bullets were suitable for a sniper rifle and controlled under ECCN 0A505.x. According to the Form BIS-711 documents filed with the DOC, these bullets had ostensibly been sold to companies in Germany, Finland, Luxembourg and Latvia, but did not disclose their ultimate re-export to Russia.

37. On or about November 24, 2022, CC-3 was again stopped by police and border guard officers in Narva, Estonia, where he was attempting to cross from Estonia into Russia. Inside of CC-3’s vehicle were approximately twenty cases of U.S.-origin bullets controlled under ECCN 0A505.x, including bullets manufactured by the Nebraska Company.

38. On or about December 6, 2022, approximately 375 pounds of U.S. ammunition was recovered from a warehouse in Estonia held in the name of CC-3’s son.



COUNT ONE  
(Conspiracy to Defraud the United States)

39. The allegations contained in paragraphs one through 38 are realleged and incorporated as if fully set forth in this paragraph.

40. In or about and between January 2017 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VADIM YERMOLENKO, together with others, did knowingly and willfully conspire to defraud the United States by impairing, impeding, obstructing and defeating, through deceitful and dishonest means, the lawful functions of OFAC and BIS, both agencies of the United States, in the enforcement of economic sanctions laws and regulations, and the issuance of licenses relating to export of goods and the provision of financial services.

41. In furtherance of the conspiracy and to effect its objects, within the Eastern District of New York and elsewhere, the defendant VADIM YERMOLENKO, together with others, did commit and cause the commission of, among others, the following:

OVERT ACTS

(a) On or about July 17, 2019, YERMOLENKO sent CC-1 electronic image files of YERMOLENKO's and YERMOLENKO's wife's signatures.

(b) On or about May 20, 2021, YERMOLENKO and CC-1 exchanged messages about a wire transaction from a Bank 2 account in the name of Strand Networks LLC. CC-1 stated, "[maybe] OFAC stopped the payment. We have to find out." CC-1 instructed YERMOLENKO to contact the bank and "[a]sk if the wire transfer was completed successfully or if there were any issues with OFAC." YERMOLENKO stated that he would "ask for a wire trace as well."

(c) On or about March 3, 2022, YERMOLENKO asked CC-1 if it was possible to “bring these things through narva [Narva, Estonia].” CC-1 responded “[u]sing the gray method—no. but let me see.”

(d) On or about June 18, 2022, CC-1 sent YERMOLENKO a DHL label to send a “token, that SIM [card] and [Bank 4] card. To Estonia.”

(e) On or about July 2, 2022, CC-1 informed YERMOLENKO, “I sent you two ACH \$1,152 from Strand Networks \$1,500 from Strandway . . . It will be required for you to go to Strand personally—[Bank 2] is asking to fill out personal and business details update.”

(f) On or about July 4, 2022, YERMOLENKO told CC-1, “I am ready now to go into [Bank 2].” CC-1 then provided YERMOLENKO with login, password and other information.

(Title 18, United States Code, Sections 371 and 3551 et seq.)

COUNT TWO  
(Conspiracy to Defraud the United States)

42. The allegations contained in paragraphs one through 38 are realleged and incorporated as if fully set forth in this paragraph.

43. On or about and between March 2019 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VADIM YERMOLENKO, together with others, did knowingly and willfully conspire to defraud the United States by impairing, impeding, obstructing and defeating, through deceitful and dishonest means, the lawful functions of the IRS in ascertainment,

computation, assessment and collection of revenue, to wit: income taxes pursuant to the Internal Revenue Code.

44. In furtherance of the conspiracy and to effect its objects, within the Eastern District of New York and elsewhere, the defendant VADIM YERMOLENKO, together with others, did commit and cause the commission of, among others, the following:

OVERT ACTS

- (a) On or about March 26, 2019, YERMOLENKO emailed CC-1 an EIN issuance letter from the IRS and Florida articles of incorporation for Squareweb LLC.
- (b) On or about August 1, 2019, YERMOLENKO opened an account for Crossgate LLC in his wife's name at Bank 2.
- (c) On or about August 2, 2019, YERMOLENKO opened accounts for Strand Networks LLC and Trailgate Systems LLC at Bank 2 and accounts for Crossgate LLC and Windwire Technologies LLC in his wife's name at Bank 3.
- (d) On or about August 5, 2019, YERMOLENKO opened an account for Fennica Networks LLC at Bank 2.
- (e) On or about August 6, 2019, YERMOLENKO opened an account for Windwire Technologies LLC in his wife's name at Bank 2.
- (f) On or about September 10, 2019, YERMOLENKO received a photograph of a Bank 2 bank card in the names of YERMOLENKO and Strand Networks LLC.
- (g) On about November 26, 2021, a Strand Networks LLC bank account received a \$49,540 incoming wire from C-R Kesha Trading and Logistics Co. Ltd.

(h) On or about April 26, 2022, YERMOLENKO opened an account in the name of “JJ Networks LLC” at a Bank 1 branch in New Jersey.

(i) On or about April 27, 2022, YERMOLENKO deposited a check for \$44,400.84 into an account in the name of “JJ Networks LLC” at a Bank 1 branch in New Jersey and immediately thereafter transferred \$9,353 to Strandway LLC and \$34,000 to Trailgate Systems LLC, before withdrawing the remaining balance in cash.

(Title 18, United States Code, Sections 371 and 3551 et seq.)

COUNT THREE  
(Bank Fraud Conspiracy)

45. The allegations contained in paragraphs one through 38 are realleged and incorporated as if fully set forth in this paragraph.

46. In or about and between January 2017 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VADIM YERMOLENKO, together with others, did knowingly and intentionally conspire to execute a scheme and artifice to defraud one or more financial institutions, and to obtain moneys, funds, credits and other property owned by, and under the custody and control of, such financial institutions by means of materially false and fraudulent pretenses, representations and promises, contrary to Title 18, United States Code, Section 1344.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNTS FOUR THROUGH SIX  
(Bank Fraud)

47. The allegations contained in paragraphs one through 38 are realleged and incorporated as if fully set forth in this paragraph.

48. In or about and between August 2019 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VADIM YERMOLENKO, together with others, did knowingly and intentionally execute schemes to defraud the financial institutions set forth below, and to obtain moneys, funds, credits and other property owned by, and under the custody and control of, such financial institutions by means of materially false and fraudulent pretenses, representations and promises.

Count	Approximate Dates	Financial Institution
FOUR	August 2019 through December 2022	Bank 2
FIVE	August 2019 through December 2022	Bank 3
SIX	April 2022 through May 2022	Bank 1

(Title 18, United States Code, Sections 1344, 2 and 3551 et seq.)

COUNT SEVEN  
(Wire Fraud Conspiracy)

49. The allegations contained in paragraphs one through 38 are realleged and incorporated as if fully set forth in this paragraph.

50. In or about and between January 2017 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VADIM YERMOLENKO, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud one or more U.S. companies by means of one or more materially false and fraudulent pretenses, representations and promises, and for

the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: electronic communications, emails and other online communications and monetary transfers in and through the Eastern District of New York and elsewhere, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT EIGHT  
(Money Laundering Conspiracy)

51. The allegations contained in paragraphs one through 38 are realleged and incorporated as if fully set forth in this paragraph.

52. In or about and between January 2017 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VADIM YERMOLENKO, together with others, did knowingly and intentionally conspire to:

(a) transport, transmit and transfer monetary instruments and funds from one or more places in the United States to and through one or more places outside the United States and to one or more places in the United States from and through one or more places outside the United States, (i) with the intent to promote the carrying on of one or more specified unlawful activities, to wit: conspiracy to violate the IEEPA and smuggling goods from the United States, contrary to Title 18, United States Code, Section 1956(a)(2)(A); and (ii) which transactions in fact involved the proceeds of unlawful activity, to wit: conspiracy to violate the IEEPA and smuggling goods from the United States, knowing that the monetary instruments and funds involved in the transportation, transmission and transfer

represented the proceeds of said unlawful activity, and knowing that such transportation, transmission and transfer was designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership and the control of the proceeds of said specified unlawful activity, contrary to Title 18, United States Code, Section 1956(a)(2)(B)(i); and

(b) engage in one or more monetary transactions, within the United States, in criminally derived property of a value greater than \$10,000 that was derived from one or more specified unlawful activities, to wit: conspiracy to violate IEEPA and smuggling goods from the United States, contrary to Title 18, United States Code, Section 1957(a).

(Title 18, United States Code, Sections 1956(h) and 3551 et seq.)

COUNT NINE  
(Conspiracy to Violate ECRA)

53. The allegations contained in paragraphs one through 38 are realleged and incorporated as if fully set forth in this paragraph.

54. In or about and between August 13, 2018 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VADIM YERMOLENKO, together with others, did knowingly and willfully conspire to violate and to cause one or more violations of licenses, orders, regulations and prohibitions issued under the Export Control Reform Act.

55. It was a part and an object of the conspiracy that the defendant VADIM YERMOLENKO, together with others, would and did agree to export and cause to be exported from the United States to Russia items on the Commerce Control List set forth in

Title 15, Code of Federal Regulations, part 774, Supplement Number 1, without having first obtained a license for such export from the U.S. Department of Commerce.

(Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G) and 4819(b); and Title 15, Code of Federal Regulations, Sections 736.2(b)(1) and 746.8(a)(1))

COUNT TEN  
(Smuggling Goods from the United States)

56. The allegations contained in paragraphs one through 38 are realleged and incorporated as if fully set forth in this paragraph.

57. In or about and between January 2017 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VADIM YERMOLENKO, together with others, did knowingly and fraudulently export and send from the United States, merchandise, articles and objects, to wit: items on the Commerce Control List set forth in Title 15, Code of Federal Regulations, part 774, Supplement Number 1, contrary to United States laws and regulations, to wit: Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G) and 4819(b) and Title 15, C.F.R. §§ 736.2 and 746.8(a)(1), and did fraudulently and knowingly receive, conceal and facilitate the transportation and concealment of such merchandise, articles and objects, prior to exportation, knowing the same to be intended for exportation contrary to such United States laws and regulations.

(Title 18, United States Code, Sections 554(a), 2 and 3551 et seq.)

CRIMINAL FORFEITURE ALLEGATION  
AS TO COUNTS ONE, TWO, SEVEN AND TEN

58. The United States hereby gives notice to the defendant that, upon his conviction of any of the offenses charged in Counts One, Two, Seven and Ten, the



government will seek forfeiture in accordance with Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which require any person convicted of such offenses to forfeit any property, real or personal, constituting, or derived from, proceeds traceable to such offenses.

59. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Section 981(a)(1)(C); Title 21, United States Code, Section 853(p); Title 28, United States Code, Section 2461(c))

**CRIMINAL FORFEITURE ALLEGATION  
AS TO COUNTS THREE THROUGH SIX**

60. The United States hereby gives notice to the defendant that, upon his conviction of any of the offenses charged in Counts Three through Six, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(2), which

requires any person convicted of such offenses, to forfeit any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such offenses.

61. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18 United States Code, Section 982(b)(1), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(2) and 982(b)(1); Title 21, United States Code, Section 853(p))

CRIMINAL FORFEITURE ALLEGATION  
AS TO COUNT EIGHT

62. The United States hereby gives notice to the defendant that, upon his conviction of the offense charged in Count Eight, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(1), which requires any person convicted of such offense to forfeit any property, real or personal, involved in such offense, or any property traceable to such property.

63. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(1) and 982(b)(1); Title 21, United States Code, Section 853(p))

CRIMINAL FORFEITURE ALLEGATION  
AS TO COUNT NINE

64. The United States hereby gives notice to the defendant that, upon his conviction of the offense charged in Count Nine, the government will seek forfeiture in accordance with Title 50, United States Code, Section 4819(d)(1), which requires any person convicted of such offense to forfeit any of the person's property: (a) used or intended to be used, in any manner, to commit or facilitate such offense; (b) constituting or traceable to the gross proceeds taken, obtained, or retained, in connection with or as a result of such offense;

and/or (c) constituting an item or technology that was exported or intended to be exported in violation of the Export Control Reform Act.

65. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be

divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 50, United States Code, Section 4819(d)(2), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 50, United States Code, Sections 4819(d)(1) and 4819(d)(2); Title 21, United States Code, Section 853(p))

A TRUE BILL

FOREPERSON

*By Carolyn Pokorny, Assistant U.S. Attorney*

BREON PEACE  
UNITED STATES ATTORNEY  
EASTERN DISTRICT OF NEW YORK